

AMENDMENTS TO THE CLAIMS:

1-8. (Cancelled)

9. (Previously presented) A method to automatically handle undesired
2 electronic mail (e-mail) in communication networks at the receiver, the method
comprising:

4 automatically comparing the sender address accompanying an incoming e-mail to
an electronically accessed list of authorized sender addresses assigned to the receiver; and
6 then

storing the e-mail in a mailbox MB of the recipient, wherein the only e-mails
8 transferred to the receiver's mailbox are those that had clearly been sent by authorized
senders;

10 in combination with:

performing an analysis to see if there is serial, incremental user identification
12 occurring so that conclusions can be drawn concerning automatic attempts at breaking into
the e-mail system.

10. (Previously presented) The method according to claim 9, wherein there
2 are two logically or physically, or both, separate mailboxes, said mailbox MB and a junk
mailbox JMB, wherein the e-mail server sends to the JMB mailbox all incoming e-mails
4 that indeed have the subscriber's correct recipient address but are not contained in the
sender list on the receiving side, thus making them available for further processing
6 selectively by the internet service provider, the administrative authorities, and by the
recipient.

11. (Previously presented) The method according to claim 9, wherein the
2 incoming e-mails are selectively put through an automatic handling and analysis process,
which can be selectively configured by the recipient and by the ISP, selectively in the e-
4 mail server, in a comparison device, and in at least one of the mailboxes, said process
initiated and configured either on a case-by-case basis or permanently.

12. (Previously presented) The method according to claim 10, wherein the
2 incoming e-mails are selectively put through an automatic handling and analysis process,
which can be selectively configured by the recipient and by the ISP, selectively in the e-
4 mail server, in a comparison device, and in at least one of the mailboxes, said process
initiated and configured either on a case-by-case basis or permanently.

13. (Currently amended) The method according to claim 9, wherein ~~all~~ when
2 executable programs are sent as attachments to e-mails, all said executable programs are
automatically separated in the JMB.

14. (Currently amended) The method according to claim 10, wherein ~~all~~ when
2 executable programs are sent as attachments to e-mails, all said executable programs are
automatically separated in the JMB.

15. (Currently amended) The method according to claim 11, wherein ~~all~~ when
2 executable programs are sent as attachments to e-mails, all said executable programs are
automatically separated in the JMB.

16. (Currently amended) The method according to claim 12, wherein ~~all~~ when
2 executable programs are sent as attachments to e-mails, all said executable programs are
automatically separated in the JMB.

17. (Previously presented) The method according to claim 9, wherein if an
2 undesired e-mail is received, discontinuation requests, or cease and desist demands, can
be generated automatically and delivered to the sender.

18-20. (Cancelled)

21. (Previously presented) The method according to claim 9, wherein virus
2 checks of the e-mail can be carried out selectively at an established time of day or each
time a message arrives.

22-24. (Cancelled)

25. (Previously presented) The method according to claim 10, wherein the
2 contents of the JMB can be cyclically deleted at specific time intervals.

26-28. Cancelled

29. (New) A method to automatically handle undesired electronic mail (e-mail) in communication networks at the receiver, the method comprising:
2 automatically comparing the sender address accompanying an incoming e-mail to
4 an electronically accessed list of authorized sender addresses assigned to the receiver; and
then
6 storing the e-mail in a mailbox MB of the recipient, wherein the only e-mails
transferred to the receiver's mailbox are those that had clearly been sent by authorized
8 senders;
in combination with:
10 performing an analysis to see if there is serial, incremental user identification
occurring, which would enable inferences to be drawn concerning automatic attempts at
12 breaking into the e-mail system that automatically try all possible codes.

30. (New) The method according to claim 29, wherein when executable
2 programs are sent as attachments to e-mails, all said executable programs are
automatically separated in the JMB.

31. (New) The method according to claim 29, wherein if an undesired e-mail
2 is received, discontinuation requests, or cease and desist demands, can be generated
automatically and delivered to the sender.

32. (New) The method according to claim 29, wherein virus checks of the e-
2 mail can be carried out selectively at an established time of day or each time a message
arrives.

33. (New) The method according to claim 29, wherein the contents of the
2 JMB can be cyclically deleted at specific time intervals.

2 34. (New) A method to automatically handle undesired electronic mail (e-mail) in communication networks at the receiver, the method comprising:
4 automatically comparing the sender address accompanying an incoming e-mail to
6 an electronically accessed list of authorized sender addresses assigned to the receiver; and
8 then
 storing the e-mail in a mailbox MB of the recipient, wherein the only e-mails
 transferred to the receiver's mailbox are those that had clearly been sent by authorized
 senders;
 in combination with:
10 performing an analysis to see if a serial, incremental change in user identification
 is occurring so that conclusions can be drawn concerning automatic attempts at breaking
12 into the e-mail system by automatically, serially, incrementally changing the user
 identification until the changed user identification matches an authorized user
14 identification.

2 35. (New) The method according to claim 34, wherein when executable
 programs are sent as attachments to e-mails, all said executable programs are
 automatically separated in the JMB.

2 36. (New) The method according to claim 34, wherein if an undesired e-mail
 is received, discontinuation requests, or cease and desist demands, can be generated
 automatically and delivered to the sender.

2 37. (New) The method according to claim 34, wherein virus checks of the e-mail
 can be carried out selectively at an established time of day or each time a message
 arrives.